#6

R E P U B L I Q U E F R A N Ç A I S E

PCT/FR99/02782

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

EJU

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

BREVET D'INVENTION

FR99/12782

REC'D 06 DEC 1999
WIPO PCT

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 26 NOV. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55-1328

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 18 NOV 1998
N° D'ENREGISTREMENT NATIONAL 98 14497
DÉPARTEMENT DE DÉPÔT 75
DATE DE DÉPÔT 18 NOV. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

AD/cb

n°du pouvoir permanent — références du correspondant: 014284 — téléphone: 01.49.69.91.91

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale: ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

Procédé de contrôle d'utilisation d'une carte à puce

3 DEMANDEUR (S) n° SIREN . . . . . code APE-NAF . . . .

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

S.C.A.
(Société en Commandite par Actions)

Nationalité (s) Française

Adresse (s) complète (s) — Pays

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS — FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL
98 14497

n° 014284

TITRE DE L'INVENTION :

Procédé de contrôle d'utilisation d'une carte à puce

LE(S) SOUSSIGNÉ(S)

Lydie BORIN
Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

VALADIER Jean-LOUIS

domicilié au : Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

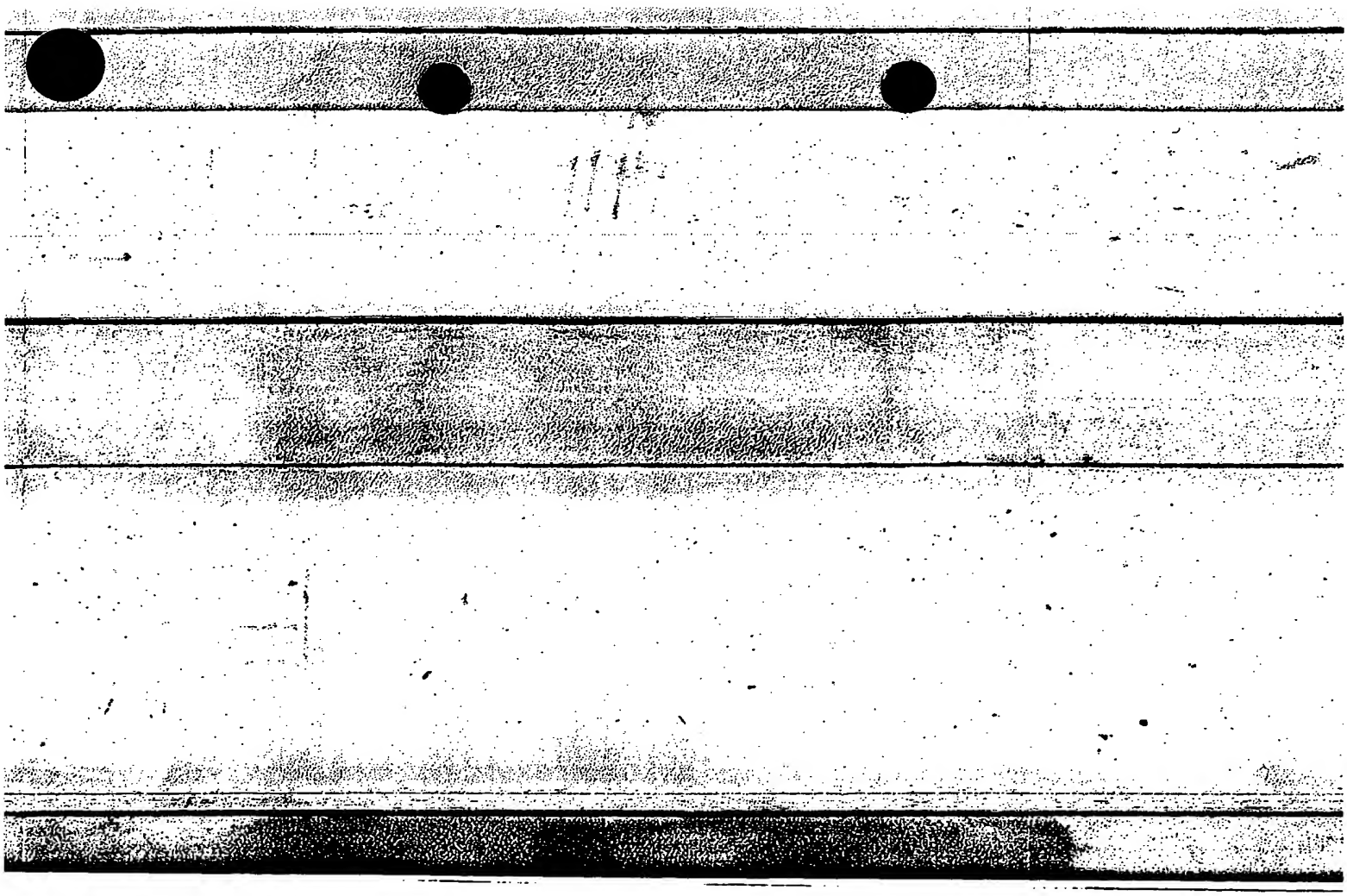
NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Fait à Cachan, le 18 novembre 1998

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

BA 113/140897



DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
15			RM	23/03/99	31 MARS 1999 - A N R

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

PROCÉDÉ DE CONTROLE D'UTILISATION D'UNE CARTE A PUCE

La présente invention concerne un procédé de contrôle d'une carte à puce.

Elle s'applique plus particulièrement aux cartes mettant en oeuvre des algorithmes de cryptographie utilisant des clés ou des couples de clés dans des sessions d'authentification, lors de transactions entre la carte et un terminal.

On entend par terminal, aussi bien le terminal dans lequel la carte est introduite, comme par exemple un terminal de paiement chez un commerçant, qu'un serveur d'une banque auquel ce terminal de paiement peut-être relié lors d'une transaction dite par liaison directe, selon un mode de transaction dit "*online*" dans la littérature anglo-saxonne. C'est notamment le cas pour les cartes bancaires (carte de débit/crédit), pour des transactions portant sur un montant qui dépasse un certain seuil et dans lesquelles le terminal se connecte automatiquement au serveur pour des vérifications supplémentaires avant d'accepter la transaction.

Dans la suite, on entend par terminal tout système extérieur auquel la carte est connectée lors d'une transaction.

L'invention s'applique notamment, mais pas exclusivement aux cartes à puce de type porte-monnaie électronique, qui sont des moyens de paiement jetables ou rechargeables.

Pour prévenir toute fraude liée à l'utilisation de cartes à puce, des algorithmes cryptographiques sont utilisés, qui utilisent des clés.

En pratique, pour un certain nombre de transactions une ou plusieurs sessions d'authentification par la carte ou par le terminal sont prévues , de manière à assurer une sécurité maximum. On entend par session d'authentification l'ensemble des opérations visant à faire calculer par la carte et par le terminal une signature (ou un certificat) correspondant à l'application d'un algorithme de cryptographie sur une donnée qui peut-être imposée par l'un ou l'autre ou un mélange de données de la carte et du terminal, et à la comparaison des deux signatures. Si cette comparaison est effectuée par la carte, c'est une authentification par la carte, qui reçoit la signature calculée par le terminal. Si c'est une authentification par le terminal, c'est le contraire.

Cependant, un nouveau type de fraude est apparue qui consiste à déduire la valeur des clés secrètes à partir d'analyses statistiques basées sur des mesures de consommation en courant de la carte, lors des périodes de calcul cryptographique. Cette méthode d'attaque, appelée attaque DPA pour *differential power analysis* repose sur le fait que l'on a des signatures de consommation en courant à partir desquelles, si on connaît au moins la donnée appliquée en entrée ou la donnée obtenue en sortie, on est capable, en faisant des hypothèses sur les clés, de retrouver la valeur ou une partie de la valeur d'une clé qui a été utilisée dans le calcul cryptographique considéré.

Pour mettre en oeuvre cette fraude, il faut donc pouvoir lancer un calcul cryptographique avec la même clé un certain nombre de fois, par exemple, 300 fois. Pour que ce soit utilisable, il faut connaître ou pouvoir imposer ou pouvoir fixer un paramètre du calcul cryptographique.

Si on prend l'exemple des cartes à puce de type porte-monnaie électronique mettant en oeuvre un

algorithme de cryptographie à clé secrète, les transactions entre une carte de ce type et un terminal se déroulent globalement selon le schéma suivant, représenté sur la figure 1 :

- dans une phase d'initialisation, la carte calcule une clé de session SKX, à partir d'une clé secrète KDX contenue dans la carte concernée et d'un compteur de sessions NTX de la carte qui est incrémenté de façon irréversible pendant la transaction.

Puis selon le type de transactions, la carte calcule une signature S1 et/ou une signature S2, en appliquant l'algorithme de cryptographie à une donnée, en général imposée par la carte, et avec la clé de session SKX.

De son côté, le terminal calcule des signatures correspondantes, et selon le type de transaction, soit le terminal est authentifié par la carte, soit la carte est authentifiée par le terminal. Il y a donc transmission de données et de signatures associées lors de sessions d'authentification.

Prenons le cas d'une tentative de fraude basée sur une transaction de type chargement (*load dans la littérature anglo-saxonne*), qui sert normalement à créditer la carte de type porte-monnaie électronique avec une certaine somme.

Si on lance un certain nombre de fois (300 fois par exemple) une transaction de ce type et si on retire la carte du terminal juste après la phase d'initialisation, le compteur de sessions NTX de la carte ne sera pas incrémenté. Si on fait 300 transactions de ce type en retirant la carte du terminal pour faire avorter la transaction, la clé de session SKX sera la même pour ces 300 transactions. On pourra donc collecter 300 courbes de mesure de consommation en courant correspondant au calcul de 300 signatures sur des données qui pourront être identiques

ou variables selon les transactions, et avec la même clé.

L'analyse statistique dans le cas où les données sur lesquelles le calcul cryptographique est appliqué, sont variables, permet d'obtenir la clé de session.

Selon le type de cartes, selon les transactions, on peut en pratique soit déduire les clés secrètes réelles contenues dans la carte, ou les clés de session.

La connaissance d'une clé secrète réelle permet d'une part de fabriquer des fausses cartes avec cette clé ; ces cartes seront vues comme bonnes par un terminal. Cette connaissance permet d'autre part de réaliser des transactions de type annulation d'achat, pour une carte de type porte-monnaie, permettant de re-créditer la carte d'un montant précédemment débité.

La connaissance d'une clé de session permet quant à elle de rejouer une transaction, en utilisant une fausse carte (un clone) ou un simulateur.

L'invention a pour objet d'empêcher ce type de fraude.

Or cette fraude nécessite deux type d'opérations distinctes:

- une opération de collection de mesures de consommation en courant, pour laquelle il faut utiliser la carte pour faire les mesures à des moments propices, avec des transactions réelles avec un terminal, mais qui sont avortées par retrait de la carte (*pull out*) ou des transactions avec un simulateur du terminal, transactions qui vont échouées par défaut d'authentification du terminal par la carte (mauvaises signatures) ; et

- une opération d'analyse statistique utilisant des moyens de simulation (ordinateurs), pour retrouver les données recherchées, c'est à dire les clés.

Pour mener à bien l'analyse statistique, il faut effectuer un grand nombre de mesures : 50, 300, 5000.

Cela veut dire que dans la carte, il va y avoir un grand nombre d'échecs de sessions d'authentifications par la carte, échecs dûs à des transactions avortées, par retrait de la carte du terminal (*pull-out*) ou échouées, par fourniture par le terminal de mauvaises signatures mauvaises signatures.

Un objet de l'invention est ainsi d'empêcher la collection de mesures de consommation en courant.

Or on a vu que dans le cas où l'on cherche à faire cette collection, on va avoir un grand nombre d'échecs de sessions d'authentification par la carte.

Une solution apportée au problème technique de l'invention consiste à utiliser dans la carte un compteur de contrôle, pour décompter (ou compter) ces échecs, et interdire l'utilisation de la carte quand un certain nombre d'échecs sont comptabilisés.

L'invention concerne donc un procédé de contrôle selon la revendication 1.

Selon l'invention, lorsqu'une transaction entre la carte et un terminal est lancée, qui utilise au moins une session d'authentification par la carte, le compteur de contrôle est décrémenté d'une unité. Il n'est ré-incrémenté de cette unité que si l'authentification est réussie. Ou bien, le compteur de contrôle est incrémenté d'une unité et n'est ensuite décrémenté de cette unité que si la session d'authentification est réussie.

De préférence, on utilise un compteur de contrôle par clé et/ou par couple de clés de cryptage utilisés dans la carte.

Le compteur de contrôle selon l'invention peut décompter depuis, ou compter jusqu'à une valeur de blocage N représentative du nombre d'échecs autorisés.

Cette valeur de blocage N dépend du type de transactions dans lesquelles la clé ou le couple de clés associé est utilisé. Cette valeur correspond à un

nombre de fois autorisé de transactions échouées ou avortées. Elle tient notamment compte du niveau de sécurité à associer à la transaction, c'est à dire du risque encouru par une fraude sur cette clé ou ce couple de clés.

Par exemple, s'agissant pour une carte de type porte-monnaie électronique, d'une transaction de mise à jour de paramètres de la carte, ces paramètres pouvant être la date d'expiration, les valeurs même des clés, un montant maximum pour une transaction ..., on prévoit une valeur N assez faible, car un très fort degré de sécurité doit être associé à une telle transaction et peu d'erreurs d'utilisation peuvent survenir pour ce type de transaction. S'agissant d'opérations d'achats ou d'annulation d'achats, pour lesquels un certain nombre d'incidents lors de l'utilisation "normale" de la carte peuvent intervenir, dûs notamment à des erreurs d'utilisation par le titulaire, on prévoit une valeur plus grande.

Pour une clé donnée ou un couple de clés donné, lorsque le compteur a atteint sa valeur limite, zéro par décrémentation ou N par incrémentation, l'utilisation de la clé ou du couple de clés est bloquée : aucune transaction utilisant cette clé ou ce couple de clés ne peut plus être effectuée. De préférence, on prévoit que ce blocage est irréversible. On peut cependant prévoir de ré-initialisiser le compteur dans le cas ou un blocage résulte indiscutablement d'une erreur non intentionnelle de l'utilisateur. On peut aussi prévoir de pouvoir modifier la valeur de blocage N, si elle se révèle en pratique trop faible ou trop grande. Ces ré-initialisation ou modification ne pourront se faire que selon une procédure très sécurisée par un tiers habilité (la banque).

En outre, dans certaines transactions, plusieurs calculs cryptographiques sont exécutés, avec la même clé ou le même couple de clés jusqu'à et y compris celui de la session d'authentification par la carte. On prévoit alors de décrémenter, ou incrémenter, le compteur ou bien d'une nouvelle unité avant chaque calcul, ou bien d'une unité représentative du nombre de calculs effectués. Si la session d'authentification est réussie, le compteur est ré-incrémenté, ou décrémenté, soit de la somme des unités décrémentées, ou incrémentées, au moyen d'un compteur de pointage ou de l'unité représentative, selon le mode d'implémentation choisi du procédé de contrôle selon l'invention.

D'autres caractéristiques et avantages de l'invention sont décrits dans la description suivante, faite à titre indicatif et nullement limitatif et en référence aux dessins annexés dans lesquels :

- la figure 1 déjà décrite représente un schéma type de calculs cryptographiques effectués lors d'une transaction entre une carte de type porte-monnaie électronique utilisant un algorithme de cryptographie à clé secrète et un terminal;
- la figure 2 est un schéma général des ressources d'une carte de ce type, comprenant des compteurs de contrôle selon l'invention; et
- les figures 3 à 5 sont des organigrammes de transactions typiques dans une application porte-monnaie électronique mettant en oeuvre le procédé de contrôle d'utilisation selon l'invention.

Le principe général de l'invention est d'utiliser au moins un compteur de contrôle que l'on va décrémenter, ou incrémenter d'une unité en début de transaction entre un terminal et une carte, et que l'on ne va ré-incrémenter, ou décrémenter qu'après une session d'authentification par la carte, si cette session est réussie.

Dans la suite on ne retient que le cas ou le compteur est décrémenté systématiquement au début de chaque transaction et ré-incrémenté sous conditions. On se transposera aisément dans le cas inverse ou le compteur est incrémenté systématiquement, en début de transaction, et décrémenté sous conditions.

Le compteur est initialisé à une valeur de blocage N, représentative du nombre d'échecs autorisés qui est notamment fonction de l'application. Si beaucoup de transactions sont démarrées sans permettre une authentification réussie par la carte, soit que la transaction ait été interrompue (cas de *pull out)*, soit que les données envoyées à la carte pour permettre l'authentification par la carte soient fausses (cas d'un simulateur utilisé à la place d'un vrai terminal), le compteur qui est décrémenté à chaque nouvelle transaction, mais qui n'est pas ré-incrémenté dans tous les cas d'échecs d'authentification par la carte, finit par atteindre zéro. L'utilisation de la carte est alors bloquée.

Un exemple de mise en oeuvre de l'invention va maintenant être expliqué pour une carte de type porte-monnaie électronique mettant en oeuvre un algorithme de cryptographie dont la clé de cryptage est une clé secrète. L'invention ne se limite pas ni à ce type de carte, ni à ce type d'algorithme. Elle s'applique à toute carte effectuant pour au moins une transaction, une session d'authentification. La session d'authentification peut utiliser un algorithme à clé secrète comme l'algorithme DES, ou un algorithme de type RSA utilisant un couple de clés de cryptage (clé privée, clé publique). Certaines cartes implémentent même ces deux algorithmes pour utiliser l'un ou l'autre selon la transaction à effectuer. Le procédé de contrôle selon l'invention s'applique à toutes ces différentes cartes et applications.

La figure 2 représente schématiquement les ressources d'une carte à puce de type porte-monnaie électronique, à laquelle on peut appliquer le procédé de contrôle de l'invention.

Elle comprend principalement un microprocesseur µP, et des ressources mémoires dont une mémoire morte ROM, contenant en pratique le code programme, une mémoire dynamique RAM comme mémoire de travail et une mémoire non volatile de type EEPROM par exemple, qui contient en pratique des paramètres sensibles (au sens sécurité) de la carte, dont des compteurs. Dans l'exemple, cette mémoire contient notamment trois clés secrètes notées KDP, KDL et KDU, trois compteurs de sessions associés, notés NTP, NTL et NTU, et trois compteurs de contrôle associés selon l'invention, notés C_{KDP}, C_{KDL}, C_{KDU}.

Cette mémoire contient d'autres paramètres. Certains peuvent être mis à jour par un système externe, par une transaction de mise à jour, selon une procédure sécurisée.

On rappelle que dans une carte porte-monnaie électronique, trois types de transactions sont possibles et à chaque type de transaction correspond une clé secrète associée. On a ainsi les types de transaction suivants :

- Achat ou annulation d'achat (*purchase or purchase cancellation)* avec la clé secrète associée, notée KDP;
- Chargement ou déchargement (*Load or Unload*) avec la clé secrète associée, noté KDL et
- Mise à jour (*update*) avec la clé secrète associée, notée KDU.

Dans l'invention, on prévoit alors d'utiliser un compteur de contrôle par clé secrète différente. On a ainsi le compteur CKDP associé à la clé secrète KDP, le compteur CKDL associé à la clé secrète KDL et le compteur CKDU associé à la clé secrète KDU.

L'exemple d'organigramme de fonctionnement d'une telle carte représenté sur la figure 3 concerne une transaction de type achat (*purchase*), pour laquelle la carte utilise donc la clé secrète KDP, le compteur de session associé NTP et le compteur de contrôle associé selon l'invention, C_{KDP}.

Une transaction d'achat comprend une première phase d'initialisation qui se limite normalement à l'envoi d'une commande par le terminal à la carte, pour lui spécifier le type de transaction. On libelle habituellement cette commande de la manière suivante, dans la littérature anglo-saxonne : *INIT FOR PURCHASE*.

Le microprocesseur se branche alors sur l'adresse du code programme correspondant à ce type de transaction.

Dans l'invention, on prévoit dans cette phase d'initialisation de décrémenter le compteur de contrôle concerné, C_{KDP}, d'une unité. La carte exécute donc l'instruction suivante : $C_{KDP} = C_{KDP} - u$.

Elle teste alors si le compteur de contrôle a atteint sa valeur limite, dans l'exemple zéro. Si il a atteint sa valeur limite ($C_{KDP} \leq 0$), la carte ne peut donner suite à la transaction, qui se terminera donc par défaut de réponse par la carte.

Si la limite n'est pas atteinte, la carte passe à une phase de traitement, dans laquelle elle procède notamment aux opérations suivantes :

- elle calcule la clé de session SK_p, en appliquant l'algorithme de cryptographie à la valeur du compteur de session NTP et en utilisant la clé secrète KDP,
- elle envoie une donnée au terminal pour qu'il calcule une signature correspondante $S2_T$,
- elle reçoit en retour la signature $S2_T$ calculée par le terminal,

- elle calcule une signature S2 en appliquant l'algorithme de cryptographie à la donnée variable envoyée au terminal, avec la clé de session SK_P.

La carte compare alors les deux signatures. Si elles sont comparables, l'authentification est réussie, le compteur de contrôle selon l'invention est alors ré-incrémenté par la valeur u. Sinon, il est inchangé. La transaction peut ensuite continuer.

On voit que si trop de transactions de type achat conduisent à un échec de l'authentification par la carte, le compteur de contrôle selon l'invention va permettre de bloquer toute utilisation de la carte pour une transaction de type achat.

En fait il bloque toute utilisation de la carte pour des transactions de même type, utilisant la même clé secrète. Ainsi, dans le cas du compteur C_{KDP}, ce sont les transactions d'achat ou d'annulation d'achat qui seront bloquées.

La figure 4 montre un organigramme de fonctionnement de la carte pour la transaction de type annulation d'achat, qui utilise donc la même clé secrète KDP.

Dans cette transaction, la phase d'initialisation initiée par une commande d'initialisation du terminal, (commande "*init for purchase cancellation*" selon la littérature anglo-saxonne), comprend, en plus de la décrémentation d'une unité u du compteur de contrôle C_{KDP} selon l'invention, le calcul de la clé de session SK_P et d'une signature S1 obtenue par application d'un algorithme de cryptographie sur une donnée, en utilisant la clé de session. A l'issue de ce calcul, la carte transmet au terminal, cette donnée et la signature S1, pour permettre au terminal d'authentifier la carte. Cette authentification par le terminal ne fait l'objet d'aucune réponse du terminal.

La carte passe à la phase de traitement dans laquelle elle authentifie à son tour le terminal, comme précédemment. Dans ce type de transaction, la signature S2 est en général calculée sur zéro. La carte calcule donc la signature S2 correspondante avec la clé de session KDP. Elle reçoit la signature $S2_T$ calculée par le terminal et effectue la comparaison des deux signatures. Si elles sont comparables, la session d'authentification est réussie. Le compteur de contrôle selon l'invention est ré-incrémenté par l'unité u. Sinon, le compteur de contrôle est inchangé. La transaction se poursuit.

Dans le cas de cette transaction, on voit que la carte effectue deux calculs cryptographiques jusqu'à et y compris celui de la session d'authentification par la carte, le calcul de la signature S1 et le calcul de la signature S2. Pour cette transaction, on prévoit alors de préférence de décrémenter le compteur de contrôle d'une valeur correspondant au nombre de calculs cryptographiques effectués jusqu'à et y compris celui de la session d'authentification par la carte.

Cette décrémentation peut se faire en une seule fois, par une unité u représentative de ce nombre de calculs réalisés pour cette transaction. La valeur prise par u pour cette transaction pourrait être initialisée dans la phase d'initialisation, suite à la commande du type *"INIT FOR"*. Cette décrémentation en plusieurs fois, en décrémentant d'une unité le compteur avant chaque calcul, dans l'exemple, avant le calcul de la signature S1 et avant le calcul de la signature S2. Dans ce cas, on prévoira de faire le test de la valeur limite sur le compteur après chaque décrémentation.

Dans ce cas aussi, on prévoit alors un compteur de pointage associé au compteur de contrôle, noté D_{KDP} sur la figure 2, initialisé à zéro au début de la transaction et que l'on vient par exemple incrémenter à

chaque fois que l'on décrémente le compteur de contrôle. Ainsi, si l'authentification par la carte est réussie, on ré-incrémente le compteur de contrôle du nombre contenu dans le compteur de pointage.

On notera que l'homme du métier utilisera l'une ou l'autre des différentes possibilités de mise en oeuvre selon les spécificités de l'application visée. Notamment on peut utiliser une mise en oeuvre pour un type de transactions et une autre pour un autre type de transactions selon le degré de sécurité voulu.

La figure 5 représente un organigramme de fonctionnement pour une autre type de transaction, celle de mise à jour. Il est relativement semblable aux précédents, mais l'authentification par la carte se fait ici sur la signature notée S1.

En fait, de manière générale, le compteur de contrôle est décrémenté au début de la transaction. Il n'est ré-incrémenté, s'il peut l'être, qu'après une session d'authentification par la carte.

On notera que les organigrammes des figures 3 à 5 ne montrent que certaines des opérations effectuées au cours de la transaction, pour l'explication du procédé selon l'invention. En pratique, d'autres opérations sont exécutées. Notamment selon les transactions, on utilise pour calculer les signatures la clé de session courante, ou la clé de session précédente. Après le calcul de la clé de session, le compteur de session doit-être incrémenté ... Tous ces aspects sont spécifiques de l'application à proprement parler et n'ont pas d'intérêt quant à la mise en oeuvre du procédé de contrôle selon l'invention.

Les différents compteurs de contrôle doivent être initialisés à une valeur de blocage N bien choisie. Cette valeur doit tenir compte du type de transactions associé, du niveau de sécurité correspondant à mettre en oeuvre mais aussi des erreurs possibles en cours

d'utilisation "normale" par le titulaire de la carte : il ne s'agit pas de bloquer l'utilisation de la carte alors que le titulaire n'a pas cherché à faire une fraude.

Dans un exemple à titre purement illustratif, mais qui rend compte des différents aspects qui doivent être pris en compte, on peut initialiser le compteur de contrôle C_{KDP} associé aux transactions achat/annulation d'achat à 100, le compteur de contrôle C_{KDL} associé aux transactions chargement/déchargement à 20, et le compteur de contrôle $C_{KD}u$ associé aux transactions de mise à jour à 10.

On a expliqué précédemment qu'une variante du procédé de contrôle selon l'invention consiste à incrémenter le compteur à chaque session et à ne le décrémenter que sous condition (authentification par la carte réussie). Dans ce cas, le compteur est initialisé à zéro, et la valeur limite, à laquelle le contenu du compteur est comparé, est égale à la valeur de blocage N. Tout ce qui a été décrit précèdemment s'applique à cette variante de l'invention.

L'invention vient d'être expliquée dans un exemple d'application à une carte porte-monnaie électronique. Mais il ressort clairement de cette description que le procédé de contrôle selon l'invention s'applique à tout type de carte à puce dès lors qu'elle réalise une session d'authentification. Cette session d'authentification peut être basée sur un algorithme de cryptographie à clé secrète, par exemple de type DES, comme expliqué dans le cas de la carte porte-monnaie électronique, mais aussi des algorithmes d'autres type, comme les algorithmes de type RSA utilisant un couple de clés (clé privée, clé publique) par exemple. Par ailleurs, dans l'invention, on entend par carte à puce aussi bien les cartes de format bien connu que des supports portables.

REVENDICATIONS

1. Procédé de contrôle de l'utilisation d'une carte à puce comprenant un microprocesseur apte à effectuer des calculs de cryptographie dans la carte pour effectuer des sessions d'authentification lors d'une transaction entre la carte et un terminal, caractérisé en ce que ledit procédé utilise au moins un compteur de contrôle (C_{KDP}) et en ce que pour une transaction comprenant au moins une session d'authentification par la carte, le procédé consiste :

- à décrémenter, ou incrémenter, d'une unité (u) le compteur de contrôle au début de la transaction et
- si l'authentification par la carte est réussie, à effectuer la ré-incrémentation, ou la décrémentation, dudit compteur de contrôle par ladite unité (u).

2. Procédé selon la revendication 2, caractérisé en ce que le compteur de contrôle peut décompter depuis, ou compter jusqu'à, une valeur de blocage.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend l'utilisation d'un compteur de contrôle par clé et/ou par couple de clés de cryptage contenus dans la carte.

4. Procédé selon la revendication 3, caractérisé en la valeur de blocage associée à un compteur est fonction du type de transactions dans lesquelles la clé associée ou le couple de clés associé est utilisé.

5. Procédé selon la revendication 3, caractérisé en ce que l'unité de décrémentation, ou d'incrémentation, d'un compteur de contrôle est représentative du nombre de calculs cryptographiques avec la clé associée ou le

couple de clés associé, effectués jusqu'à et y compris celui de ladite session d'authentification pendant ladite transaction.

6. Procédé selon la revendication 3, caractérisé en ce que le compteur de contrôle associé à une clé ou un couple de clés est décrémenté, ou incrémenté, d'une nouvelle unité, avant chacun des calculs cryptographiques utilisant ladite clé ou le dit couple de clés, jusqu'à et y compris celui de ladite session d'authentification par la carte.

7. Procédé selon la revendication 5, caractérisé en ce que la ré-incrémentation, ou la décrémentation, du compteur par l'unité représentative du nombre de calculs cryptographiques est effectuée si la session d'authentification par la carte est réussie.

8. Procédé selon la revendication 6, caractérisé en ce qu'il comprend un compteur de pointage (D_{KDP}) pour mémoriser le nombre de décrémentations, ou d'incrémentations, d'une unité effectuées, pour permettre la ré-incrémentation, ou la décrémentation, du compteur de contrôle (C_{KDP}) par le contenu du compteur de pointage, si la session d'authentification par la carte est réussie.

9. Procédé de contrôle selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite session d'authentification par la carte est effectuée lors d'une connexion par liaison directe à un serveur.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que, lorsque le compteur de contrôle est décrémenté, ou

incrémenté, jusqu'à une valeur limite, il bloque l'utilisation de la clé associée ou du couple de clé associé.

11. Procédé selon la revendication 10, caractérisé en ce que le blocage de l'utilisation de la clé ou du couple de clés est irréversible.

12. Carte à puce comprenant au moins un compteur de contrôle associé à au moins une clé et/ou un couple de clés pour la mise en oeuvre d'un procédé de contrôle selon l'une quelconque des revendications précédentes.

feuille rectifiée

REVENDICATIONS

1. Procédé de contrôle de l'utilisation d'une carte à puce comprenant un microprocesseur apte à effectuer des calculs de cryptographie dans la carte pour effectuer des sessions d'authentification lors d'une transaction entre la carte et un terminal, caractérisé en ce que ledit procédé utilise au moins un compteur de contrôle (C_{KDP}) et en ce que pour une transaction comprenant au moins une session d'authentification par la carte, le procédé consiste :

- à décrémenter, ou incrémenter, d'une unité (u) le compteur de contrôle au début de la transaction et
- si l'authentification par la carte est réussie, à effectuer la ré-incrémentation, ou la décrémentation, dudit compteur de contrôle par ladite unité (u).

2. Procédé selon la revendication 1, caractérisé en ce que le compteur de contrôle peut décompter depuis, ou compter jusqu'à, une valeur de blocage.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend l'utilisation d'un compteur de contrôle par clé et/ou par couple de clés de cryptage contenus dans la carte.

4. Procédé selon la revendication 3, caractérisé en la valeur de blocage associée à un compteur est fonction du type de transactions dans lesquelles la clé associée ou le couple de clés associé est utilisé.

5. Procédé selon la revendication 3, caractérisé en ce que l'unité de décrémentation, ou d'incrémentation, d'un compteur de contrôle est représentative du nombre de calculs cryptographiques avec la clé associée ou le

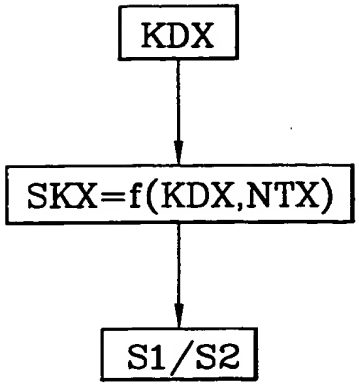

KDX
SKX=f(KDX,NTX)
S1/S2

FIG.1

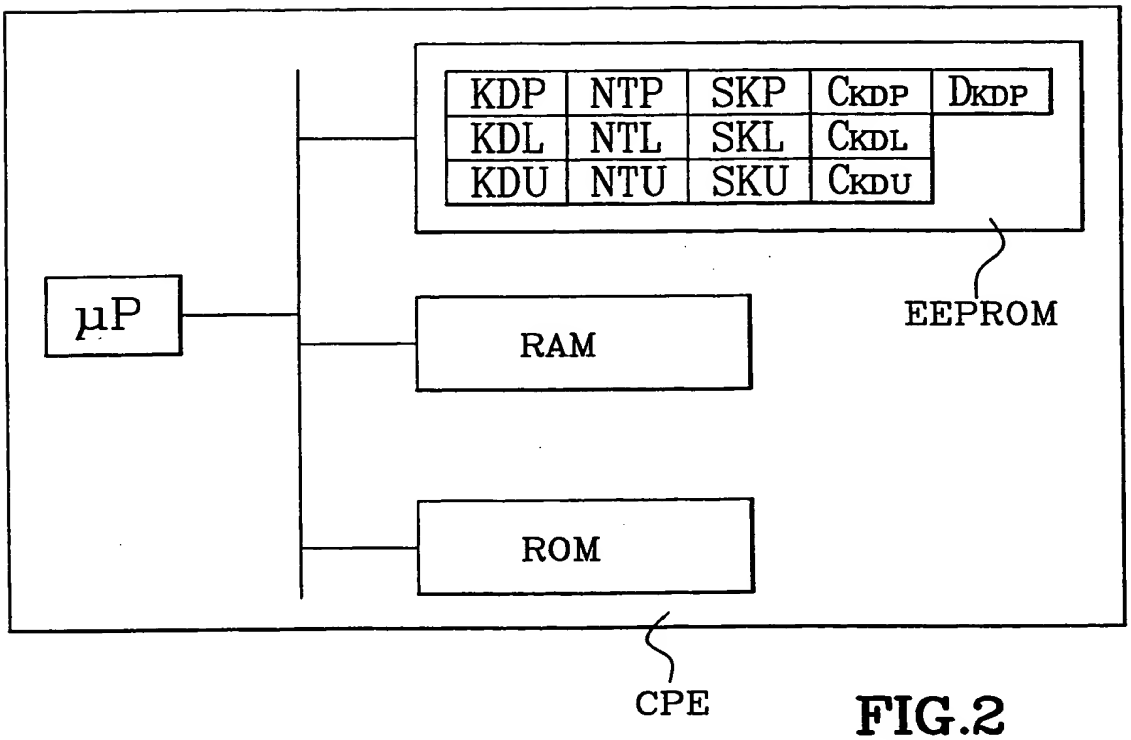

KDP
NTP
SKP
CKDP
DKDP
KDL
NTL
SKL
CKDL
KDU
NTU
SKU
CKDU
EEPROM
µP
RAM
ROM
CPE

FIG.2

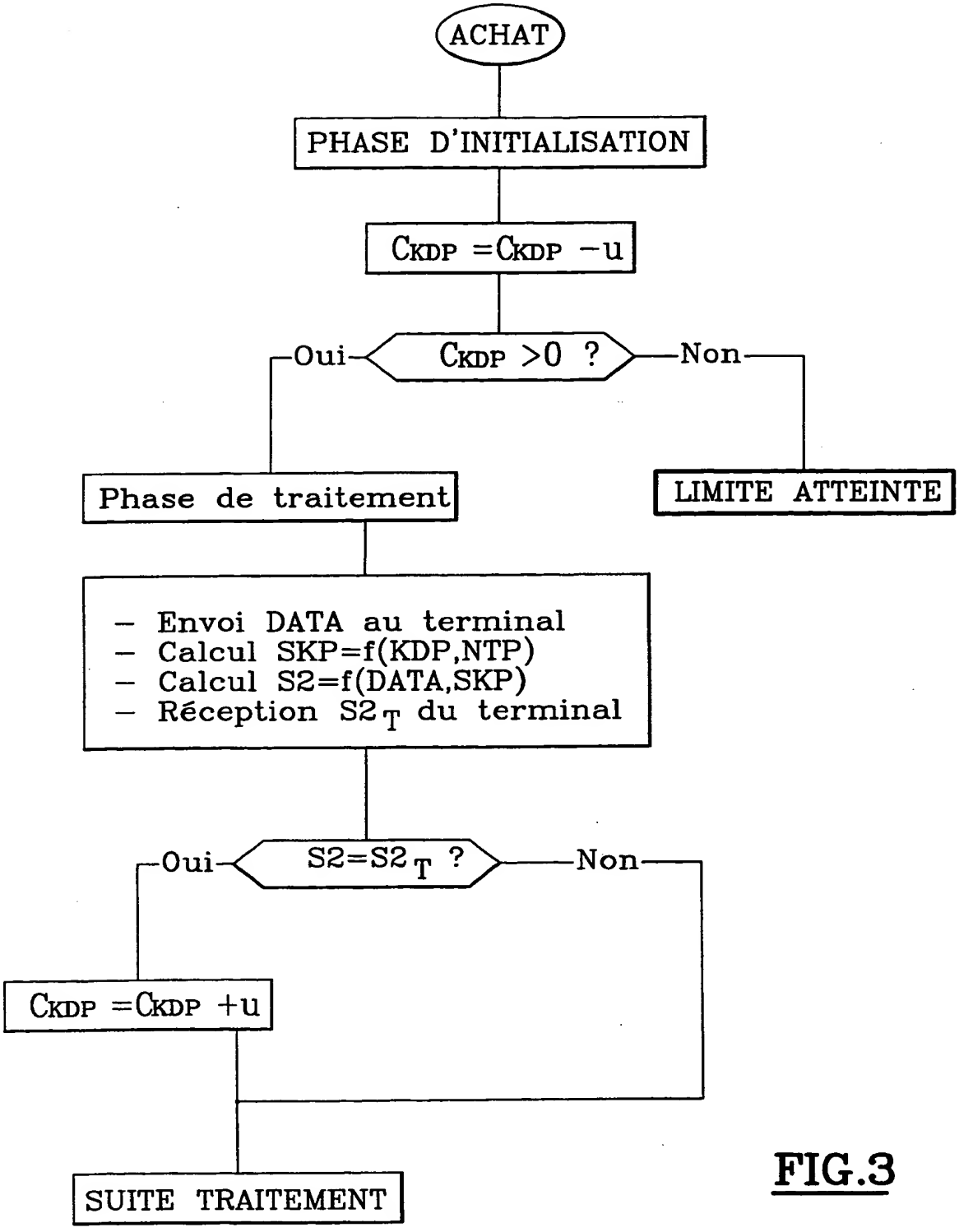

ACHAT
PHASE D'INITIALISATION
CKDP =CKDP -u
Oui
CKDP >0 ?
Non
Phase de traitement
LIMITE ATTEINTE
- Envoi DATA au terminal
- Calcul SKP=f(KDP,NTP)
- Calcul S2=f(DATA,SKP)
- Réception S2T du terminal
Oui
S2=S2T ?
Non
CKDP =CKDP +u
SUITE TRAITEMENT

FIG.3

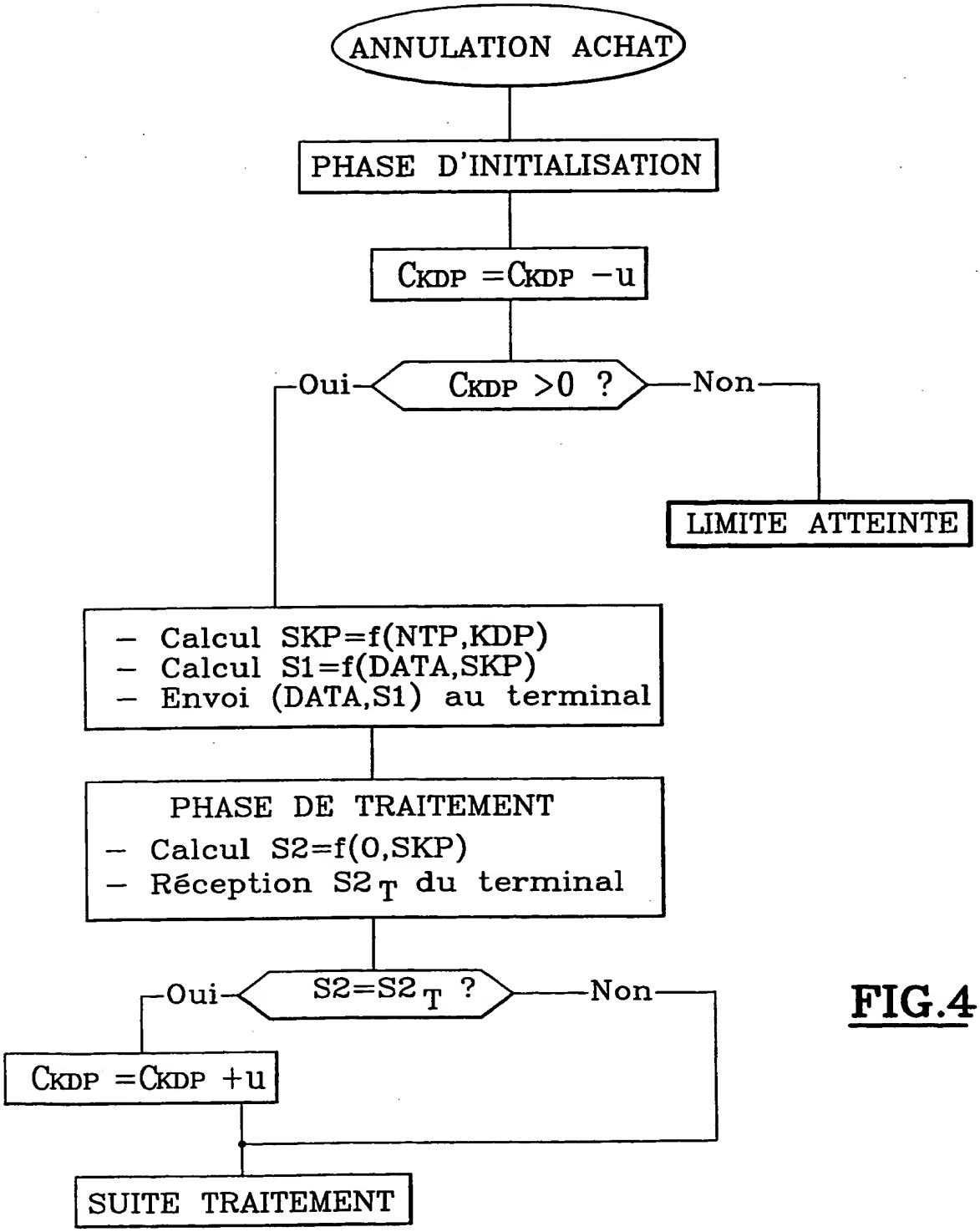

ANNULATION ACHAT
PHASE D'INITIALISATION
CKDP =CKDP −u
Oui
CKDP >0 ?
Non
LIMITE ATTEINTE
– Calcul SKP=f(NTP,KDP)
– Calcul S1=f(DATA,SKP)
– Envoi (DATA,S1) au terminal
PHASE DE TRAITEMENT
– Calcul S2=f(0,SKP)
– Réception S2T du terminal
Oui
S2=S2T ?
Non
CKDP =CKDP +u
SUITE TRAITEMENT

FIG.4

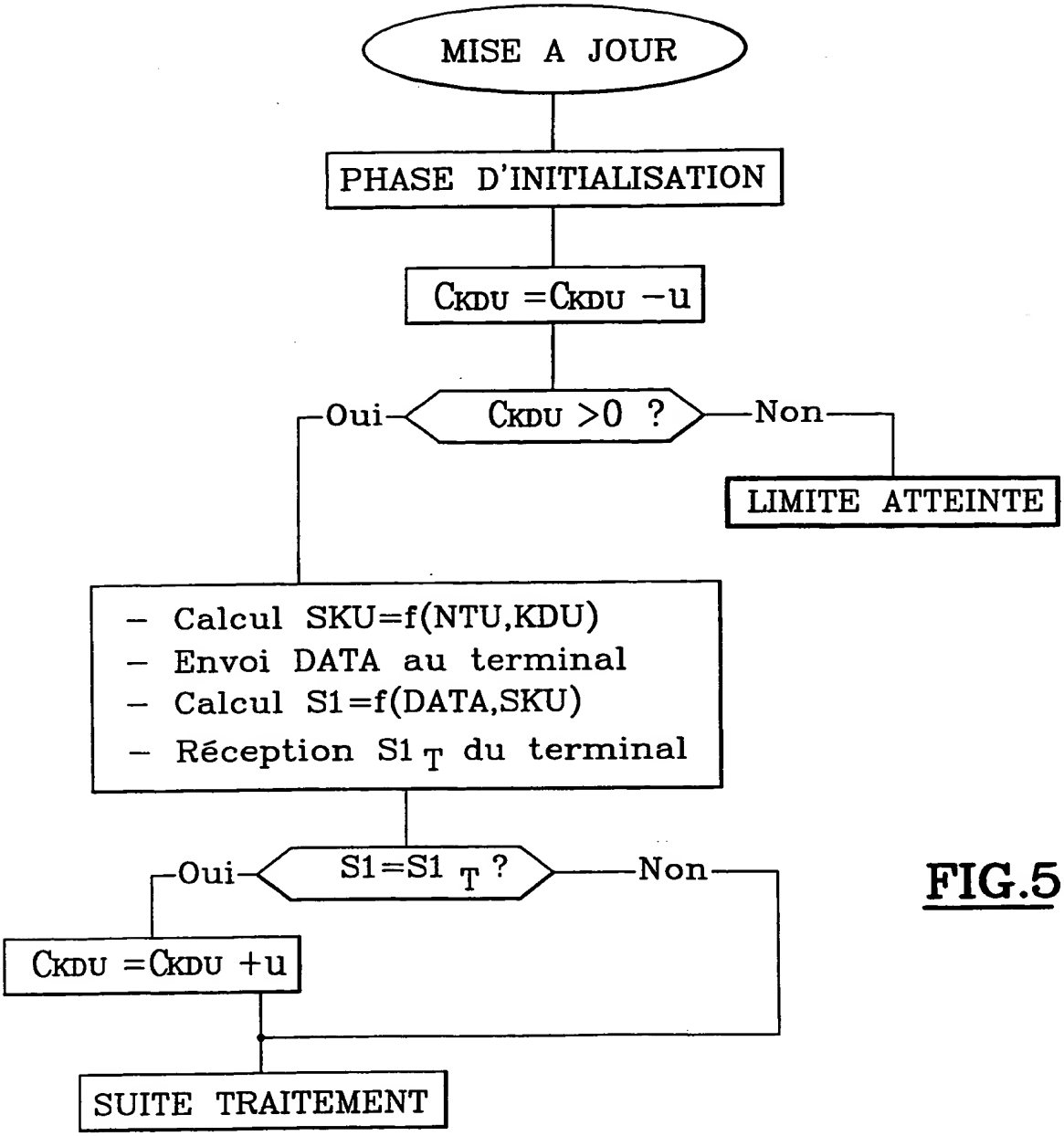

MISE A JOUR
PHASE D'INITIALISATION
CKDU =CKDU -u
Oui
CKDU >0 ?
Non
LIMITE ATTEINTE
- Calcul SKU=f(NTU,KDU)
- Envoi DATA au terminal
- Calcul S1=f(DATA,SKU)
- Réception S1 T du terminal
Oui
S1=S1 T ?
Non
CKDU =CKDU +u
SUITE TRAITEMENT

FIG.5